COVER PAGE

Hewlett-Packard Company Docket Number:

10019968-1

Title:

System and Method for Secure Data Transmission

Inventor:

Neal A. Krawetz
4736 Westbury Dr.
Fort Collins, Colorado 80526

SYSTEM AND METHOD FOR SECURE DATA TRANSMISSION

TECHNICAL FIELD OF THE INVENTION

The present invention relates generally to the field of data processing and, more particularly, to a system and method for secure data transmission.

BACKGROUND OF THE INVENTION

The Internet has become a popular avenue for transferring data. However, a considerable amount of data transferred via the Internet may be of a sensitive or confidential nature. Thus, sensitive or confidential data transferred via the Internet is oftentimes encrypted for protection and authenticated using a certificate generally issued by a certificate authority. However, encrypted data transfers and certificates suffer several disadvantages. For example, secure socket layers (SSL) use time-based certificates. Because the set time at each end of the data transfer may be different, for example, between a sender and a server, valid certificates may be incorrectly expired or expired certificates may be inadvertently accepted. Web browsers may be configured to prompt a user of an invalid certificate. However, many users may simply accept the certificate without understanding the purpose of the certificate or the consequences of accepting an invalid certificate. Additionally, automated senders generally require a hard-coded response. Accordingly, if an invalid certificate is accepted, the data transfer may be subject to third party interception. Furthermore, if the certificate is rejected, a determination must generally be made regarding where to obtain a valid certificate.

SUMMARY OF THE INVENTION

In accordance with one embodiment of the present invention, a method for secure data transmission comprises generating a character string at a sender, generating a hash key using the character string and a private key, and encrypting the data using the hash key. The method also comprises transmitting an identification key associated with the sender, the character string, and the encrypted data from the sender to a recipient.

In accordance with another embodiment of the present invention, a system for secure data transmission comprises a processor, a memory coupled to the processor, and a string generator stored in the memory and executable by the processor. The string generator is adapted to generate a character string. The system also comprises a hashing engine stored in the memory and executable by the processor. The hashing engine is adapted to generate a hash key using the character string and a private key. The system further comprises an encryption engine stored in the memory and executable by the processor. The encryption engine is adapted to encrypt the data using the hash key. The processor is adapted to transmit the encrypted data, an identification key related to the private key, and the character string to a recipient.

In accordance with yet another embodiment of the present invention, a method for secure data transmission comprises receiving a character string and an identification key from the sender. The method also comprises receiving encrypted data from the sender. The method further comprises determining a private key associated with the sender using the identification key and decrypting the encrypted data using the private key and the character string.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

FIGURE 1 is a diagram illustrating a system for secure data transmission in accordance with an embodiment of the present invention;